What is claimed is:

1. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site, the secondary virtual file server needing resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site, a method comprising:

a) determining whether there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing user access at the disaster recovery site; and

b) upon finding that there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing user access at the disaster recovery site, reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site.

2. The method as claimed in claim 1, wherein the primary file server is a virtual file server.

3. The method as claimed in claim 1, which is performed when it is desired to perform a configuration change of the primary file server at the active site, and which includes performing a configuration change of the primary file server at the active site.

after reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site once the configuration change of the primary file server at the active site has been performed.

4. The method as claimed in claim 1, which is performed when it is desired to failover user access from the active site to the disaster recovery site, and which includes performing failover of user access from the active site to the disaster recovery site after reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site after failover of user access from the active site to the disaster recovery site.

5. The method as claimed in claim 1, wherein user mappings are kept at the disaster recovery site so that user file access at the active site may be continued by accessing user file copies at the disaster recovery site upon failover of user access from the active site to the disaster recovery site.

6. The method as claimed in claim 1, wherein a primary copy of user mappings is kept at the disaster recovery site, and a read-only cache of the user mappings is kept at the active site.

7 The method as claimed in claim 1, wherein user session information is kept at the disaster recovery site so that users accessing user files of the primary file server at the active site may access copies of the user files at the disaster recovery site without a need

to log onto the disaster recovery site upon failover of user access from the active site to the disaster recovery site.

8. The method as claimed in claim 1, wherein a network client accessing the primary file server at the active site detects a failure of the primary file server to respond to a file access request in a timely fashion, and upon detecting the failure of the primary file server to respond to the file access request in a timely fashion, the network client redirects the file access request to the disaster recovery site.

9. The method as claimed in claim 8, wherein the network client accesses the primary file server using a CIFS connection, and the network client detects the failure of the primary file server to respond to the file access request in a timely fashion and redirects the file access request to the disaster recovery site without terminating the CIFS connection.

10. The method as claimed in claim 1, which includes the disaster recovery site producing and storing a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a consistent state for the secondary virtual file server.

11. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site, the secondary virtual file server needing

resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site, a method comprising:

a) determining whether there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site once a configuration change would be made to the primary file server; and

b) upon finding that there are insufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site once the configuration change would be made to the primary file server, providing an operator with a list of missing resources or discrepancies, and receiving from the operator a choice of termination or configuration change; and

c) upon receiving from the operator a choice of configuration change, reserving network interfaces and file system mounts that are available and needed at the disaster recovery site for providing user access at the disaster recovery site once the configuration change would be made to the primary file server; and then

d) performing the configuration change to the primary file server.

12. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site, the secondary virtual file server needing

resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site, a method comprising:

a) determining whether there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site; and

b) upon finding that there are insufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site, providing an operator with a list of missing resources or discrepancies, and receiving from the operator a choice of termination or forced failover; and

c) upon receiving from the operator a choice of forced failover, reserving network interfaces and file system mounts that are available and needed at the disaster recovery site for providing user access at the disaster recovery site; and then

d) performing failover of user access from the active site to the disaster recovery site.

13. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site, a method comprising:

maintaining a primary copy of user mappings at the disaster recovery site and a read-only cache of the user mappings at the active site during user file access at the active site; and

upon failover of user access from the primary file server at the active site to the virtual secondary server at the disaster recovery site, accessing the primary copy of user mappings at the disaster recovery site in order to continue user file access at the disaster recovery site.

14. The method as claimed in claim 13, wherein user session information is kept at the disaster recovery site so that users accessing files of the primary file server at the active site may continue to access copies of the files at the disaster recovery site without a need to log onto the disaster recovery site upon failover of user access from the active site to the disaster recovery site.

15. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site, a method comprising:

maintaining a copy of user session information at the disaster recovery site during user file access at the active site; and

upon failover of user access from the primary file server at the active site to the virtual secondary server at the disaster recovery site, accessing the copy of the user session information at the disaster recovery site so that users accessing files of the primary file server at the active site continue to access copies of the files at the disaster recovery site without a need to log onto the disaster recovery site.

16. The method as claimed in claim 15, wherein a network client accessing the primary file server at the active site detects a failure of the primary file server to respond to a file access request in a timely fashion, and upon detecting the failure of the primary file server to respond to the file access request in a timely fashion, the network client redirects the file access request to the disaster recovery site.

17. The method as claimed in claim 16, wherein the network client accesses the primary file server using a CIFS connection, and the network client detects the failure of the primary file server to respond to the file access request in a timely fashion and redirects the file access request to the disaster recovery site without terminating the CIFS connection.

18. The method as claimed in claim 15, which includes the disaster recovery site producing and storing a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a consistent state for the secondary virtual file server.

19. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site, a method comprising:

a network client accessing the primary file server at the active site using a CIFS connection and detecting a failure of the primary file server to respond to a file access request in a timely fashion, and upon detecting the failure of the primary file server to

respond to the file access request in a timely fashion, the network client redirecting the file access request to the disaster recovery site without terminating the CIFS connection.

20. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the primary file server storing a collection of user files, and the secondary virtual file server storing secondary copies of the user files, the method comprising:

replicating changes to the user files from the primary file server to the secondary copies of the user files in the secondary virtual file server during user file access at the active site; and

during the replication of the changes to the user files from the primary file server to the secondary virtual file server, creating at the disaster recovery site a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a group consistent state of the user files in the secondary virtual file server.

21. A disaster recovery system comprising:

a primary file server at an active site; and

a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files that have been replicated from the primary file server to the disaster recovery site, the secondary virtual file server needing resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site,

wherein the disaster recovery system is programmed for responding to a request from a system administrator by:

a) determining whether there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing user access at the disaster recovery site; and

b) upon finding that there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing user access at the disaster recovery site, reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site.

22. The system as claimed in claim 21, wherein the primary file server is a virtual file server.

23. The system as claimed in claim 21, which is programmed for performing a configuration change of the primary file server at the active site after reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site once the configuration change of the primary file server at the active site has been performed.

24. The system as claimed in claim 21, which is programmed for performing failover of user access from the active site to the disaster recovery site after reserving the network interfaces and file system mounts that are needed at the disaster recovery site for

providing user access at the disaster recovery site after failover of user access from the active site to the disaster recovery site.

25. The system as claimed in claim 21, which is programmed for keeping user mappings at the disaster recovery site so that user file access at the active site may be continued by accessing user file copies at the disaster recovery site upon failover of user access from the active site to the disaster recovery site.

26. The system as claimed in claim 21, which includes storage at the disaster recovery site containing a primary copy of user mappings, and which includes a read-only cache of the user mappings at the active site.

27. The system as claimed in claim 21, which is programmed for keeping user session information at the disaster recovery site so that users accessing user files of the primary file server at the active site may access copies of the user files at the disaster recovery site without a need to log onto the disaster recovery site upon failover of user access from the active site to the disaster recovery site.

28. The system as claimed in claim 21, which includes a network client programmed to detect a failure of the primary file server to respond to a file access request in a timely fashion, and upon detecting the failure of the primary file server to respond to the file access request in a timely fashion, to redirect the file access request to the disaster recovery site.

29. The system as claimed in claim 28, wherein the network client is programmed for accessing the primary file server using a CIFS connection, and for detecting the failure of the primary file server to respond to the file access request in a timely fashion and redirecting the file access request to the disaster recovery site without terminating the CIFS connection.

30. The system as claimed in claim 21, wherein the disaster recovery site is programmed for producing and storing a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a consistent state for the secondary virtual file server.

31. A disaster recovery system comprising:

a primary file server at an active site; and

a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files that have been replicated from the primary file server to the disaster recovery site, the secondary virtual file server needing resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site,

wherein the disaster recovery system is programmed for responding to a configuration change request from a system administrator by:

a) determining whether there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing

unrestricted user access at the disaster recovery site once a configuration change would be made to the primary file server; and

b) upon finding that there are insufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site once the configuration change would be made to the primary file server, providing the system administrator with a list of missing resources or discrepancies, and receiving from the operator a choice of termination or configuration change; and

c) upon receiving from the operator a choice of configuration change, reserving network interfaces and file system mounts that are available and needed at the disaster recovery site for providing user access at the disaster recovery site once the configuration change would be made to the primary file server; and then

d) performing the configuration change to the primary file server.

32. A disaster recovery system comprising:

a primary file server at an active site; and

a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files that have been replicated from the primary file server to the disaster recovery site, the secondary virtual file server needing resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site,

wherein the disaster recovery system is programmed for responding to a failover request from a system administrator by:

a) determining whether there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site; and

b) upon finding that there are insufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site, providing the system administrator with a list of missing resources or discrepancies, and receiving from the operator a choice of termination or forced failover; and

c) upon receiving from the operator a choice of forced failover, reserving network interfaces and file system mounts that are available and needed at the disaster recovery site for providing user access at the disaster recovery site; and then

d) performing failover of user access from the active site to the disaster recovery site.

33. A disaster recovery system comprising:

a primary file server at an active site; and

a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site;

wherein the disaster recovery system is programmed for:

maintaining a primary copy of user mappings at the disaster recovery site and a read-only cache of the user mappings at the active site during user file access at the active site; and

upon failover of user access from the primary file server at the active site to the virtual secondary server at the disaster recovery site, for accessing the primary copy of user mappings at the disaster recovery site in order to continue user file access at the disaster recovery site.

34. A disaster recovery system comprising:

a primary file server at an active site; and

a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site;

wherein the disaster recovery system is programmed for:

maintaining a copy of user session information at the disaster recovery site during user file access at the active site; and

upon failover of user access from the primary file server at the active site to the virtual secondary server at the disaster recovery site, accessing the copy of the user session information at the disaster recovery site so that users accessing files of the primary file server at the active site continue to access copies of the files at the disaster recovery site without a need to log onto the disaster recovery site.

35. The system as claimed in claim 34, which includes a network client programmed for accessing the primary file server at the active site and for detecting a failure of the primary file server to respond to a file access request in a timely fashion, and upon

detecting the failure of the primary file server to respond to the file access request in a timely fashion, for redirecting the file access request to the disaster recovery site.

36. The system as claimed in claim 35, wherein the network client is programmed for accessing the primary file server using a CIFS connection, and upon detecting the failure of the primary file server to respond to the file access request in a timely fashion, for redirecting the file access request to the disaster recovery site without terminating the CIFS connection.

37. The system as claimed in claim 36, wherein the disaster recovery site is programmed for producing and storing a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a consistent state for the secondary virtual file server.

38. In a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site, a system comprising:

a network client accessing the primary file server at the active site using a CIFS connection and detecting a failure of the primary file server to respond to a file access request in a timely fashion, and upon detecting the failure of the primary file server to respond to the file access request in a timely fashion, the network client redirecting the file access request to the disaster recovery site without terminating the CIFS connection.

39. A disaster recovery system comprising:

a primary file server at an active site;

a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site; and

at least one network client programmed for accessing the primary file server at the active site using a CIFS connection and detecting a failure of the primary file server to respond to a file access request in a timely fashion, and upon detecting the failure of the primary file server to respond to the file access request in a timely fashion, redirecting the file access request to the disaster recovery site without terminating the CIFS connection.

40. The disaster recovery system as claimed in claim 39,

wherein said at least one network client includes a CIFS redirection agent for passing CIFS requests from said at least one network client to the primary file server, the CIFS redirection agent having a timer for detecting the failure of the primary file server to respond to the file access request in a timely fashion, and

wherein the primary file server includes a CIFS connection maintenance agent for ensuring that a timely response to each CIFS request is returned to said at least one network client, the CIFS connection maintenance agent having a timer for determining whether the CIFS connection maintenance agent needs to return a response to said each CIFS request for maintaining the CIFS connection.

41. A disaster recovery system comprising a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the primary file server storing a collection of user files, and the secondary virtual file server storing secondary copies of the user files, wherein the system is programmed for replicating changes to the user files from the primary file server to the secondary copies of the user files in the secondary virtual file server during user file access at the active site, and wherein the disaster recovery site is programmed for creating at the disaster recovery site a series of snapshot copies of the secondary virtual file server during the replication of the changes to the user files from the primary file server to the secondary virtual file server, each of the snapshot copies providing a group consistent state of the user files in the secondary virtual file server.